WE CLAIM

1. A computer security system, comprising:

a terminal security access device connected to a computer and configured to prohibit access to the computer upon detecting an unauthorized access attempt and to maintain data security and integrity on the computer;

said terminal security access device determining access to the computer by checking operations selected from the group consisting of passwords, fingerprint readers, biometric sensors, and electronic surveillance systems;

said terminal security access device maintaining data security by embedding encrypted security codes with the data, by transferring the data in encrypted form at all times, by providing copies of the data exclusively in encrypted form, and by enabling transfer of the data to another computer only if the other computer is equipped with a similar security system.

2. The computer security system according to claim 1, wherein said terminal security access device comprises at least one component having a self-destruct feature, such that when the self-destruct feature is triggered, access to the computer is denied.

3. The computer security system according to claim 1, wherein the computer is configured in one or more networks and the system further comprises an added communications security system.

4. The computer security system according to claim 3, wherein said communications security system is a multi-level process of transferring data from one location to another electronically within the network, a first level utilizing the encrypted data and a second level formed with security-enhanced modems.

5. The computer security system according to claim 4, wherein said security-enhanced modems are provided with at least one component having a self-destruct feature.

6. A method of providing access security to a computer system, which comprises the following method steps:

providing a computer access security system enabled to allow or deny access to a computer;

initializing the computer access security system upon an initial system startup, by assigning personal access code numbers for each administrator of the computer access security system, assigning an initial terminal security code, and allocating limited access storage space for receiving audit and access data;

upon receiving a request for administrator access the computer system, prompting for user input of the personal access code number and subsequently verifying the personal access code number;

storing in the access storage space all successful and unsuccessful access attempts and accesses to the computer system; and

subsequent to the initial setup of the computer system, continuing with a sequence of operations starting with computer user login.

7. The method according to claim 6, which further comprises periodically transmitting with a computer security access device to a terminal security access device a new randomly generated terminal identification number.

8. The method according to claim 7, which comprises transmitting the terminal identification number in encrypted form.